contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Acer Connect M6E 5G Portable WiFi Router: new CVE

CVE-2026-128791 · record published 24 November 2026

Analysis Report

Anyone running the Acer Connect M6E 5G on firmware from M6E_AI_1.00.000019 to M6E_GBL_1.00.000079 should update immediately; the record scores this 10 out of 10. Apply the over-the-air update to …

PREPARED BY	NamiQ	DATE	24 November 2026
FACTS AS OF	24 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/acer-connect-m6e-5g-portable-wifi-router-cve-2026-128791

The bottom line

> *Anyone running the Acer Connect M6E 5G on firmware from M6E_AI_1.00.000019 to M6E_GBL_1.00.000079 should update immediately; the record scores this 10 out of 10. Apply the over-the-air update to M6E_GBL_1.00.000107 from the router's settings now.*

At a glance

Fact	Detail
Product	Acer Connect M6E 5G Portable WiFi Router (CVE-2026-128791)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by Acer on 24 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 24 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	M6E_GBL_1.00.000107, available via over-the-air update — stated in the CVE record.
Who looks first	Anyone who has deployed the Acer Connect M6E 5G Portable WiFi Router on firmware between M6E_AI_1.00.000019 and M6E_GBL_1.00.000079, wherever other devices share the WiFi.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you use an Acer Connect M6E 5G Portable WiFi Router?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware between M6E_AI_1.00.000019 and M6E_GBL_1.00.000079 (inclusive)?	Nothing to do for this CVE.	Apply the OTA update to M6E_GBL_1.00.000107 immediately.
Do other devices — laptops, phones, guest devices — share this router's WiFi?	Risk is lower, but the update still applies.	Any of those devices could trigger the deletion; update before the next session.

What it is

Any device already connected to the router's WiFi can send a single unauthenticated HTTP request to permanently delete files — no login, no special account, nothing else needed.

Why it matters

CWE-306 means the router's file-deletion endpoint requires no credentials at all — no login screen, no token. Any device on the WiFi can call it. The record scores this 10 out of 10. Our reading is that meeting recordings are the files most at risk, given the endpoint path name; a device present in a session could remove all recordings silently before anyone notices. The record's remediation text recommends immediate application of the update now available via OTA.

Things people will get wrong

- Only attackers outside the network can exploit this. The record says any WiFi client can send the request. The attacker is already on the WiFi — no external access path is needed.
- The router must be internet-facing for this to matter. The flaw requires only WiFi access. Any device already connected — including guest or compromised ones — can trigger the deletion without crossing an external boundary.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on your router

- Log in to the router's web management interface and locate the firmware or system information page; the version string will be in the M6E_ format described in the record.
- Compare against the affected range: M6E_AI_1.00.000019 through M6E_GBL_1.00.000079.

Step 2: Reduce exposure while the update is arranged

- Restrict which devices can connect to the WiFi until the update is applied; a smaller set of trusted clients reduces who can send the unauthenticated request.

Step 3: Apply the OTA firmware update

- The record states M6E_GBL_1.00.000107 is available now via over-the-air update; apply it from the router's firmware update or system settings page.
- After the update completes, confirm the version shown matches M6E_GBL_1.00.000107.

Step 4: Confirm no files were unexpectedly deleted

- Review any meeting recordings stored on or through the router; the endpoint path in the record suggests these are the files at risk.
- If recordings are missing that you expected to be present, preserve any available router logs before resetting or updating.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are writing about a security flaw in the Acer Connect M6E 5G Portable WiFi Router, CVE-2026-128791, published 24 November 2026. The flaw allows any device on the router's WiFi to permanently delete files without any login. The affected firmware range is M6E_AI_1.00.000019 through M6E_GBL_1.00.000079. The fixed version is M6E_GBL_1.00.000107, available via over-the-air update. Please let us know whether we run this router, which firmware version is installed, and whether the OTA update has been applied. We would like written confirmation of the firmware version and the fix by 1 December 2026.*

The weakness behind it

The record classes this as CWE-306.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Data Destruction (T1485): Deleting or overwriting data so it cannot be recovered.	Impact: causing damage or disruption	The flaw directly enables permanent, unauthenticated file deletion; this would typically map to data destruction as the primary impact.

Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The router exposes an HTTP endpoint any network client can reach without credentials; exploiting it would likely follow the pattern of exploiting a network-accessible application interface.
File and Directory Discovery (T1083): Listing files and folders to find what is there.	Discovery: looking around	Before deleting, an attacker would likely probe related paths to discover what files are present; file and directory discovery would typically precede the deletion step.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *Any WiFi client can send HTTP DELETE to /meeting-recording/delete to permanently delete files without authentication.*

Versions of Acer Connect M6E 5G Portable WiFi Router the record lists as affected:

- M6E_AI_1.00.000019 through M6E_GBL_1.00.000079

The record gives no version ranges. Use the vendor's advisory for the affected versions.

What the record says to do about it, in the vendor's words:

> *These vulnerabilities have been resolved in firmware version M6E_GBL_1.00.000107, which is available now via an over-the-air (OTA) update. It is strongly recommended to apply this patch immediately.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-128791
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-128791
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not say which file types or directories are reachable via the deletion endpoint, beyond what the path name suggests.
- It is not stated whether the router logs HTTP DELETE requests, or whether any log would survive if the deletion endpoint was called.
- The remediation text in the record refers to 'these vulnerabilities' in the plural; the other flaws fixed in M6E_GBL_1.00.000107 are not named in the record.
- No source states whether the OTA update requires an active internet connection or can be applied from a locally downloaded file.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 24 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-128791: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
24 November 2026	CVE record published by Acer.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Router on affected firmware used in a meeting or recording session with multiple WiFi clients present	High	Update before the next use

Router on affected firmware deployed in a shared space where guest or unmanaged devices connect	High	Update immediately
Router on affected firmware used as a personal hotspot with trusted devices only	Medium	Update this week
Router running firmware M6E_GBL_1.00.000107 or confirmed not in the affected range	None	No action needed for this CVE

Appendix 4. Definition of done

- Every Acer Connect M6E 5G Portable WiFi Router you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-128791: https://www.cve.org/CVERecord?id=CVE-2026-128791
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: community.acer.com: https://community.acer.com/en/en/kb/articles/20236-security-advisory-firmware-update-for-acer-connect-m6e-5g-portable-wi-fi-router